International Journal of Applied Engineering
Research and Development (IJAERD)
ISSN(P): 2250-1584; ISSN(E): 2278-9383
Vol. 4, Issue 2, Apr 2014, 49-56

TRANS STELLAR
• Journal Publications • Research Consultancy

SECURITY MECHANISMS FOR SMARTPHONES: SURVEY

DIKSHA KALE[1], VIJAY BHOSALE[2] & SUDHIR SAWARKAR[3]

[1]Department of Computer M. E, MGM College of Engineering and Technology, Navi Mumbai, Maharashtra, India

[2]Department of Computer, MGM College of Engineering and Technology, Navi Mumbai, Maharashtra, India

[3]Department of Computer, Datta Meghe College of Engineering, Maharashtra, India

ABSTRACT

Smartphones has emerged as most popular gadget nowadays. Smartphones provide most of functionalities of personal computers and also has developing features and applications based on internet, due to which smartphones becomes more vulnerable to security threats such as virus, worm, Trojans etc. Smartphones are constrained by storage, battery, processing so it is difficult to implement high security services on the smartphone itself. Another new technology gaining attraction today is cloud computing providing better resource utilization and improved scalability. This paper proposes a review on examining different existing architectures providing security for Smartphones.

KEYWORDS: Android, Cloud Computing, Security Mechanisms, Smart Phones, Threats

INTRODUCTION

Smartphones

Today, Smartphones are most popular communication devices. They come with a feature such as web browsing capability, facility to download and run software application from internet. They come with high processing power, bigger screen size and extra storage as compared to traditional mobile phones.

As architecture of such devices are much similar to traditional personal computers in terms of functionality as well as performance, common security threats like worms, Trojans and viruses are also affecting smart phones. Most of the attackers, targets Smartphones because various new applications are continuously being developed for the smartphones that are easily available and can be downloaded from internet, through which attackers can inject malicious code into smartphones.

To protect from such threats some security algorithms required that used to secure desktop-PC. But these algorithms are highly complex and resource consuming, and can't be executed on Smartphones as they have power, computational and storage limitations.

Another problem is inconsistency in software support and security fixes by the manufacturer of smartphone device. If bug fixes and patches are not provided by manufacturers to customers then security of smartphone would be highly compromised and make them vulnerable to attack. Most of Security check algorithms are proposed on signature based behavior detection, where database of signatures need to be updated frequently and also has huge database size. So implementing such detection techniques on smartphones is very difficult and expensive.

Cloud Computing

A new computing prototype which gives hosted services by sharing resources which are accessible over internet

and exploiting concept of dynamic scalability has emerged in Cloud Computing. Cloud computing provides services for computation, storage, data access, security and software that does not require end-user knowledge of the physical location and configuration of the system that delivers the services.

The concept of cloud computing provides three service models: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Within these three service models, consumers are provided with ready to use Software (in SaaS), development and runtime environments (in PaaS), and resources such as CPU, memory, and data storage as a service (in IaaS)[1].

This paper analyses different approaches that provides security mechanisms for smartphones based on cloud services.

Smartphone Security

Smartphone security can be considered in various aspects such as types of threats, infection channels and security functions that can be applied to protect the smartphones as shown in figure 1.

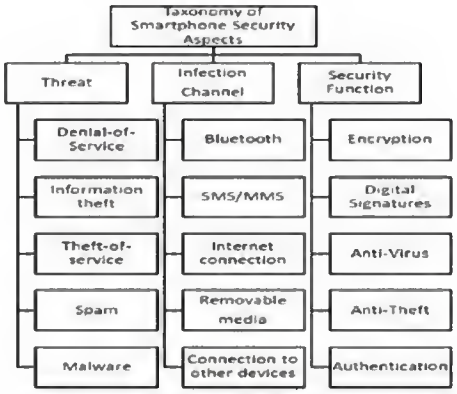

Figure 1: Taxonomy of Smartphone Security [7]

Threats

Denial-of-Service Attack

This attack throws a large number of packets to the device to exhaust the battery or to consume other resources such as memory, CPU cycles, port numbers, etc

Information Theft

Attacker tries to obtain private information from the smartphone such as users sensitive data stored on it or temporary information such as phone location, BlueSnarfing and Bluebugging attack are examples of information theft.

Theft-of-Service

Smartphone resources are consumed by malware such as sending huge number of messages. Mosquito virus is an example where illicit copies of a computer game were infected with a virus sending expensive SMS messages when the game was played by users.

Spam

Mobile users are targeted to receive huge number of advertising messages or similar messages. Bluejacking

utilizes a Bluetooth device name to advertise a message which other users discover when searching for Bluetooth devices.

Malware

Examples of one specific type of malware on smartphones called trojans are Skulls, Metal Gear, and Gavno.

Infection Channels

Bluetooth

Viruses spread through Bluetooth. The most well-known virus of this kind is Cabir.

SMS or MMS

These are used by smartphone viruses to spread within networks, e.g. by attaching a copy of itself on to a SMS or MMS message and sending it to another device. A good example of a worm which browses the Smartphone's contacts and then spreads via MMS is Commwarrior.

Internet Connection

Smartphones using Wi-Fi, GPRS, 3G Network access can attach to internet. Downloading files such as Skulls and Doomboot, concealed as games, smartphones can be infected by a virus.

Removable Media

An example of malware is the Windows Trojan Delf propagated via SD card of a Samsung S8500 Wave smartphone [7].

Connection to Other Devices

If we are connecting our mobile to PC or any other mobile device then during this synchronization, a virus can penetrate the smartphone. Example is Crossover virus.

Security Function

Encryption

Most widely used encryption algorithms are Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) .Now smartphone provides encryption for data stored on it. Blackberry providing encryption for data stored on media cards, Microsoft's' introduction of its Encrypted File System (EFS), Nokia's Wallet application, Apple's hardware encryption for the iPhone 3GS, and LUKS for Android phones.

Digital Signatures

Verify authenticity of messages sent and of the sender. Digital signatures can also be used to verify integrity, as any changes to the message after it has been digitally signed will invalidate the signature. Furthermore, digital signatures can be used to sign applications.

Anti-Virus Software

It can be used to discover, avoid, and eliminate malware such as viruses, worms, Trojan horses, spyware, etc. from the smartphone. A common method for malware detection is signature scanning where known patterns of malware in executable code and files are searched for.

Anti-Theft Security

In case of stolen or lost devices, protects data of smartphones. One such method is remote wiping of data from a smartphone. This method has both legal risks and the risk of becoming an attack vector itself. Another method is to remotely lock access to the Smartphone's data.

Authentication

Ensure that only approved users are able to access functions and data of a smartphone. For higher security requirements more advanced and stronger authentication mechanisms such as two factor authentication, behavior based authentication, voice recognition, and key stroke based authentication can be used Smartphones .

LITERATURE REVIEW

Virtualized in-Cloud Security Services for Mobile Devices [2]

Model proposed by Oberheide has a mobile antivirus functionality, moved to a network which works parallel on multiple virtualized malware detection engines. Lightweight mobile host agent and network service are the two main components of this architecture. The former, works on mobile devices, analyses by acquiring files and send them back to the network which is then received by network service that identifies the malicious content. The main benefits of this model are device resource consumption is reduced by computation offloading; device software complexity is reduced and thirdly better detection. A prototype for this model is developed for Nokia N800 and N95 devices running Symbian OS. They show that their approach is feasible and effective for the current generation of Smartphone.

Paranoid Android: Versatile Protection for Smartphone's [3]

Prototype proposed by Portokalis et al consist of a remote security server that conducts the security checks and has exact replica of the phone in virtual environments, called as Paranoid Android. By allowing us to enjoy multiple detection techniques simultaneously, servers are not subjected to any kind of constraints of similarity. To replay the actions of the real smartphone in the replicas this method uses the previously recorded system traces. Including anti-virus scans and dynamic taint checking the remote server can perform security scans on the replicas.

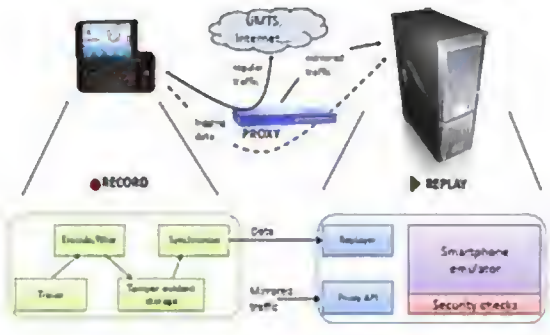

Figure 2: Paranoid Android Architecture [3]

Battery life is reduced by about 30% and the transmission overhead can be kept below 2.5 KiBps, were the two main evaluation of this prototype. The authors explain how the battery consumption could be improved significantly and conclude that the architecture is suitable for protection of mobile phones.

A Cloud-Based Intrusion Detection and Response System for Mobile Phones [4]

A response architecture and cloud-based intrusion detection was proposed by Houmansadr et al. real time plus accurate detection and response, light resource usage and transparent operations to the user are its main objectives. By emulating a smartphone in the cloud this architecture uses a proxy to duplicate the traffic between internet and the smartphone. Detection systems and resource intense off-the-shelf intrusion forensics makes intrusion detection possible on the emulated smartphone. The system replicates the user's input in the cloud to keep the device and the emulated device synchronized. On detection of any malicious activity the best countermeasure is taken upon and is send to the device by the architecture automatically. A prototype of the forensics engine in the cloud uses a set of intrusion detection systems and the logging of system calls to analyze the installed application.

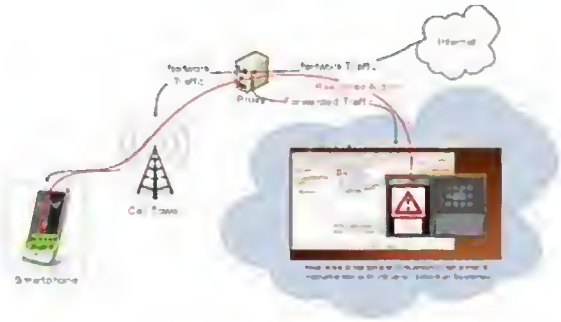

Figure 3: System Architecture for Cloud Based IDS for Smartphones [4]

Applying Behavioral Detection on Android-Based Devices [5]

A Host-based Intrusion Detection System (HIDS) is realized by behavioral-based framework called Andromaly for Android Smartphone's was presented by Shabtai A. and Elovici Y. Classifying according to their maliciousness and monitoring various features and events on the smartphones, the detection system directly runs on the device. The evaluation of their framework is done by testing game and tool application in which the classification algorithm is able to distinguish between those two kinds of applications.

The authors evaluate several combinations of classification algorithms and feature selections and conclude that the proposed anomaly detection is feasible on Android devices.

Crowdroid: Behavior-Based Malware Detection System for Android [6]

Framework for obtaining and analyzing Smartphone application activities called Crowdroid was put forwarded by Burguera et al.Analysis of the system calls of application on the Smartphone's of many users at a center server by this framework. To differentiate between benign applications and their corresponding malware versions is the main scope of this framework. Applications are not only installed from the internet but also from the official application market there are chances that the copies of malicious application with added malware functionality. Burguera et al. show that their framework is a promising approach to distinguish between a benign application and the corresponding malicious version.

COMPARATIVE ANALYSIS

By analyzing various Security systems for android smartphones we can classify these systems based on various mechanisms as below.

Table 1: Comparative Analysis of Various Security Systems for Android Smartphones

Author	Approach	Detection Method	Platform	Description
Jon Oberheide 2008	HIDS,NIDS	Signature based behavior detection	Android OS	Mobile antivirus functionality is moved to an off-device network service employing multiple virtualized malware detection engines. Provides better detection, reduced on device software complexity.
Portolakidis Et al.(2010)	HIDS,NIDS	Anomaly Detection	Android OS	A remote security server in the cloud performs the Malware detection analysis. Virtual environments will be used to mobile phone replicas analyze Android.
Amir Houmansadr.(2011)	HIDS,NIDS	Behavior based Detection	Android OS	Proxy Server is responsible for duplicating traffic between smartphone and internet. On Emulator multiple detectors detects misbehavior and system attack graphs are generated. Makes use of game Theoretic optimization for optimal response.
Shabtai et al.(2011)	HIDS	Anomaly Detection	Android OS	Host-based malware detection system that continuously monitors smartphone features and events and applies machine learning to classify the collected data as normal (benign) or abnormal (malicious) based on already known malware and behavior.
Burguera (2011)	NIDS	Behavior based Detection	Android OS	Based on dynamic analysis of application behavior to detect malware in the Android platform. The detector collects traces from an unlimited number of real users based on crowdsourcing

CONCLUSIONS

This paper surveys multiple security services for Smartphone's, which offloads the detection of malicious applications from the Smartphone into the cloud. Approach proposed by Jon Oberheide [2], Amir Houmansadr [4], Burguera [6] works on behavior based detection whereas, Portolakidis [3], Shabtai[5] works on anomaly detection but every author used android OS as platform.

REFERENCES

1. Michael Miller, "Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online", 800 East 96th Street, Indianapolis, Indiana 46240.
2. Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn, and Farnam Jahanian. Virtualized In-Cloud Security Services for Mobile Devices. In Workshop on Virtualization in Mobile Computing (Mobi Virt '08),

Breckenridge, Colorado, June2008

3. Georgios Portokalidis, Philip Homburg, Kostas Anagnostakis, and Herbert Bos. Paranoid android: versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference, 2010
4. Amir Houmansadr, Saman A. Zonouz, and Robin Berthier. A cloud-based intrusion detection and response system for mobile phones. In Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and NetworksWorkshops, DSNW '11, pages 31–32, Washington, DC, USA, 2011. IEEE Computer Society
5. Asaf Shabtai and Yuval Elovici. Applying behavioral detection on android-based devices. In MOBILWARE, pages 235–249, 2010.
6. Iker Burguera, Urko Zurutuza, and Simin N. Tehrani. Crowdroid: behavior-based malware detection system for Android. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM '11, pages 15–26, New York, NY, USA, October 2011. ACM.
7. Philipp Stephanow Lakshmi Subramanian, Gerald Q. Maguire Jr. An architecture to provide cloud based security services for smartphones, 2011.
8. Mr. Vishal S. Patil1, Mr. Sushant A. Patinge, Mr. Chetan J. Shelke. Enhanced Secured Cloud Oriented Detection Mechanism for Android Applications. Volume 3, Issue 11, November 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.